Strategy Research Project

NETWORK REQUIREMENTS IN SUPPORT OF ARMY'S LANDWARNET TRANSFORMATION

BY

COLONEL CHRIS MILLER
United States Army

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
02-15-2011	Strategy Research Project	

4. TITLE AND SUBTITLE
Network Requirements in Support of Army's LandWarNet Transformation

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Chris Miller

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel David Collins
Department of Distance Education

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

To overcome the challenges of future requirements for information dominance, the Army must develop a strategy that ensures organizations have access to global networks and required services throughout any area of operation. This research project analyzes the Army's transformation of the LandWarNet in support of an expeditionary Army engaged in persistent conflict. This paper identifies how well the Army has formally identified requirements for its Continental United States (CONUS) Network Enterprise Centers (NECs) and evaluates the plan for resourcing the minimum essential capabilities required to meet the demands of the CONUS based operational Army.

15. SUBJECT TERMS
Network Enterprise Centers, Command, Control, Communications, Computers, and Information Management (C4IM)

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	26	

USAWC STRATEGY RESEARCH PROJECT

NETWORK REQUIREMENTS IN SUPPORT OF ARMY'S LANDWARNET TRANSFORMATION

by

Colonel Chris Miller
United States Army

Colonel David Collins
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Chris Miller

TITLE: Network Requirements in Support of Army's LandWarNet Transformation

FORMAT: Strategy Research Project

DATE: 15 February 2011 WORD COUNT: 5,009 PAGES: 26

KEY TERMS: Network Enterprise Centers, Command, Control, Communications, Computers, and Information Management (C4IM)

CLASSIFICATION: Unclassified

To overcome the challenges of future requirements for information dominance, the Army must develop a strategy that ensures organizations have access to global networks and required services throughout any area of operation. This research project analyzes the Army's transformation of the LandWarNet in support of an expeditionary Army engaged in persistent conflict. This paper identifies how well the Army has formally identified requirements for its Continental United States (CONUS) Network Enterprise Centers (NECs) and evaluates the plan for resourcing the minimum essential capabilities required to meet the demands of the CONUS based operational Army.

NETWORK REQUIREMENTS IN SUPPORT OF ARMY'S LANDWARNET TRANSFORMATION

> We're building an Army that is a versatile mix of tailorable and networked organizations operating on a rotational basis…to provide a sustained flow of trained and ready forces for full spectrum operations…and to hedge against unexpected contingencies… at a tempo that is predictable and sustainable for our all volunteer force.
>
> —General George W Casey, Jr.,
> Chief of Staff of the United States Army

The United States (U.S.) military's fundamental purpose is to wage or deter war.[1] The employment of networks is becoming a critical strategic enabler for the entire military. The Department of Defense's (DoD) ability to counter violent extremists is only one critical area of emphasis that is essential for success. It is clear to the President, the Secretary of Defense (SECDEF) and the majority of Soldiers in uniform that the Army must be prepared to wage war on traditional battlefields, and in all domains (Air, Land, Sea, Space and Cyber) while simultaneously addressing asymmetrical threats to the United States in both space and cyberspace. The 2010 National Security Strategy (NSS) states "space and cyberspace capabilities that power the daily lives and military operations are vulnerable to disruption and attack."[2] As a result, DoD must do everything in its power to protect the networks. Additionally, the NSS directs all governmental agencies and departments to pursue new strategies to protect against attacks and challenges to the cyber networks that we all depend upon.[3] DoD currently has a "federation" of dozens of networks that support its Armed Forces. It sometimes refers to them with a plural tense and sometimes as they are a singular one. For the purpose of this paper, the singular term network refers to that federation.

One major response to this critical requirement and executive level directives, DoD established U.S. Cyber Command (CYBERCOM), and each Military Service created its own component command to assist with the management and defense of networks. “By statute and Presidential Directive, the Department of Homeland Security (DHS) has the lead for the Federal Government to secure civilian government computer systems, to work with industry, to defend privately-owned and operated critical infrastructure, and to secure their information systems.”[4] Many different civilian companies and communications providers assist the DoD by providing network connectivity for military locations. Networks availability and reliability are enhanced through the planning, integrating, coordinating, and oversight by several organization including Strategic Command (STRATCOM), Cyber Command (USCYBERCOM), Defense Information System Command, (DISA), and Network Technology Command (NETCOM).

“Rapid technological improvements in cyber capabilities, combined with the low cost of obtaining them, allow states and, non-state actors to threaten and disrupt military, economic, and other digital networks anywhere in the world.”[5] DOD and Joint Doctrine mandate that organizations must achieve and maintain unity of effort within the Joint Force, the U.S Government, and the international community to gain and improve operational capabilities.[6]

Dynamic changes in technology have created challenges and opportunities for Joint Force Commanders (JFC), yet maintaining dominance in all domains on land, air, sea, space and cyberspace is essential at every level. Additionally, a commander’s ability to operate and maneuver in and through cyberspace is critical to an

organization's capability to accomplish its mission. "Cyberspace and its associated technologies offer unprecedented opportunities for the United States and are vital to national security and, by extension, to all aspects of military operations."[7]

In their ongoing endeavors, to achieve unity of effort, DoD and other U.S. agencies face challenges by the multiple heterogeneous networks they utilize. In addition to personnel deployed in Iraq and Afghanistan, the U. S. has over 600 thousand personnel stationed in the Continental United States (CONUS) on military installations, in small satellite recruiting stations, and other government facilities. Each of these locations relies on connectivity to the network, which provides voice and data to conduct daily operations and support forward deployed operational forces. Currently, there are many network challenges at Army's posts, camps and stations, which affect the ability of U.S. military personnel's ability to fight upon arrival. Aging and failing equipment, local infrastructure problems, operations and policy, and a lack of qualified personnel, all create concerns for the deploying commanders.

This paper addresses the CONUS based Generating Force in support of those who rely on the networks to conduct operations. The Global Network Enterprise Construct (GNEC) is the Army wide strategy that will transform the LandWarNet to an enterprise activity. "Under GNEC, the desired LandWarNet end-state configuration is composed of three major components: the global defense network, post/camp/station campus area networks, and deployed networks."[8] In 2009, the Chief of Staff of the Army (CSA) directed the Army signal leadership to continue to develop the enterprise and LandWarNet using the Global Network Enterprise Construct (GNEC). "GNEC is best described as the focused, time-phased, resource-sensitive, Army-wide (Active, Reserve

and National Guard) strategy to transform the LandWarNet from many loosely affiliated independent networks into a truly global capability that functions like a single integrated enterprise. GNEC supports four strategic objectives: 1) enabling warfighting capabilities through the networks; 2) dramatically improving network defense; 3) realizing efficiencies while improving the effectiveness; and 4) ensuring interoperability with DoD."[9] GNEC is the Army's effort to manage all service networks and applications as a single effort. Several stated goals from GNEC include enhanced mobility, cost savings and improved security. Additionally, GNEC purports to allow units to use some of their garrison functions and applications while deployed. The network enterprise center (NEC) personnel operate and maintain the post/camps/stations campus area networks. The NEC organizations were the former Director of Information Management (DOIM) personnel assigned to provide network services. This paper will outline the proposed future NEC organizations, missions and a recommendation for change to the C4IM services catalog.

With the ever-changing computer Information technology (IT) requirements, the responsible command and organization has changed multiple times. Information System Command (ISC) was the initial proponent but because of the proliferation of the networks, ISC passed the responsibility to the local garrisons and the DOIMs to manage. NECs are now under the operational control of the 7th Signal Command. In 2009, the Army approved a name change for the DOIMs and now the new organization is designated NEC. The NEC operating construct provides a strategy for an Army validation process on all requirements on the CONUS installations.

Army Regulation, Networks Design, Organizational Structure, and Services

Army Regulation (AR) 25-1 provides guidance for Information Management, Army Knowledge, and Information Technology. This is the driving force for network implementation. The regulation sets forth the requirement for Command, Control, Communications, Computers and Information Management (C4IM) catalog. The Army proponent for implementation and change management of Information Management (IM) is the Army's Chief Information Officer (CIO) G6. The publication of the C4IM services catalog defines network services and designates them as "Baseline" or "Mission" services. Baseline services are common services such as telephone or Non-Classified Internet Protocol Router Network (NIPR) electronic mail (EMAIL) connectivity.[10] Department of the Army budgets for, manages and distributes the funding to pay for the baseline communications services. Local commands who have funds reimburse the NEC for unfunded common baseline services or additional command mission unique services. Mission services require a reimbursement from the requester to pay for the service ordered. An example is an additional video teleconference circuit for a unit conference room over and above the C4IM catalog authorization.

The Army network design is to deploy an integrated network, which spans all echelons of command and supports Army, Joint and Coalition operations.[11] This support will encompass both operating and generating forces and will continue to support the Army Force Generation (ARFORGEN) cycle. The Army's goal is to deliver IT services that are relevant and affordable in support of operations. The LandWarNet is the Army's solution to the enterprise network requirement and contribution to the global information grid (GIG).[12]

The Army Chief of Staff approved the global network enterprise construct (GNEC) as the network enterprise strategy for the Army. As part of the GNEC strategy, the Army leadership in March 2008 assigned a single commander with responsibility for networks service in CONUS. 7th Signal Command was activated in March 2009 with two strategic brigades for CONUS.

The 7th Signal Command is responsible for all networks on Army installations and assumed oversight of 37 NECs within CONUS. The NECs are organizations on Army installations that are responsible for the delivery of Information technology services that include voice, data, and video. The command was to achieve the spirit of the original single DOIM initiative by transitioning disparate IT operations, and consolidating the command and control of all Army NEC operations in accordance with the Army campaign plan. The Army conducted multiple inspections, which identified multiple networks operating outside of a single IT provider. The designated organization responsible delivery of the IT services is the NEC.

Prior to the formation of the 7th Signal Command, the Army established the director of information management (DOIM) to deliver specialized IT services as required on each installation. The Army approved a transition of the DOIM organizations to the Installation Management Command (IMCOM) in early 2000, along with all resources. This transition was part of a move to position all services on an installation under one command, and an attempt to gain efficiencies and improve command and control. However, IMCOM did not have the required technical expertise or oversight capability, so the requirement fell on the Regional Chief Information Operations (RCIO) under Network Technology Command (NETCOM).

The RCIOs had oversight responsibility, but had limited resources to assist the DOIMs. DOIM organizations were responsible for delivering the IT services required by regulation in direct support of senior commanders on installations. This caused each DOIM to provide services and meet different standards within their limited resources of money and personnel. As a result, many DOIMs struggled and pursued the additional resources required to complete their missions. The Army than developed a single DOIM action plan, directed by the Chief of Staff of the Army, which transferred the resources required to provide C4IM services to the DOIMs. DOIMs were subsequently renamed Network Enterprise Centers (NECs) as part of the transition to the new 7th Signal Command.

AR25-1 designates the network enterprise centers (NECs) as the only organizations in CONUS authorized to provide common use baseline services on a non-reimbursable basis to all installation tenants, as prescribed by the C4IM services list. Services provided by the NECs include telephone, Cell Phone, VTC, network security support, data network services, email services, computer and peripheral devices, and website development and maintenance. Currently, the funding level allocated by the Army for common user services are at the amber or red level. That is between 60 and 80 percent on average. Further complicating this situation is the fact that some organizations request services at the enhanced common user level. This requires increased service levels or extended service requirements far above the common user services. The cost of these enhanced services exceeds current common user service funding. Enhanced common user services are separate and unique from the above-mentioned services, and provide more specific, secure and specialized capability to

military units, requiring specialized personnel and equipment. All of these services come with additional resource and funding requirements.

Network enterprise centers (NECs) are the organizations in the Continental United States (CONUS) that provide network and services to users on each post, camp and stations. The NECs are under the operational control of 7th Signal Command, the theater-level command that is responsible for providing resourcing and oversight.

The NECs scalable organization structure is dependent upon the type, size, and unique mission of the supported installation. Three different NEC structures accomplish the communications missions in CONUS today. The three-division structure is the base structure. The base structure is scalable to five divisions, which have a business and plans division, networking and switching division, system support division, desktop support division and information assurance division. This structure is scalable based on the size and number of personnel on each of the installations. See Figure 1.[13]

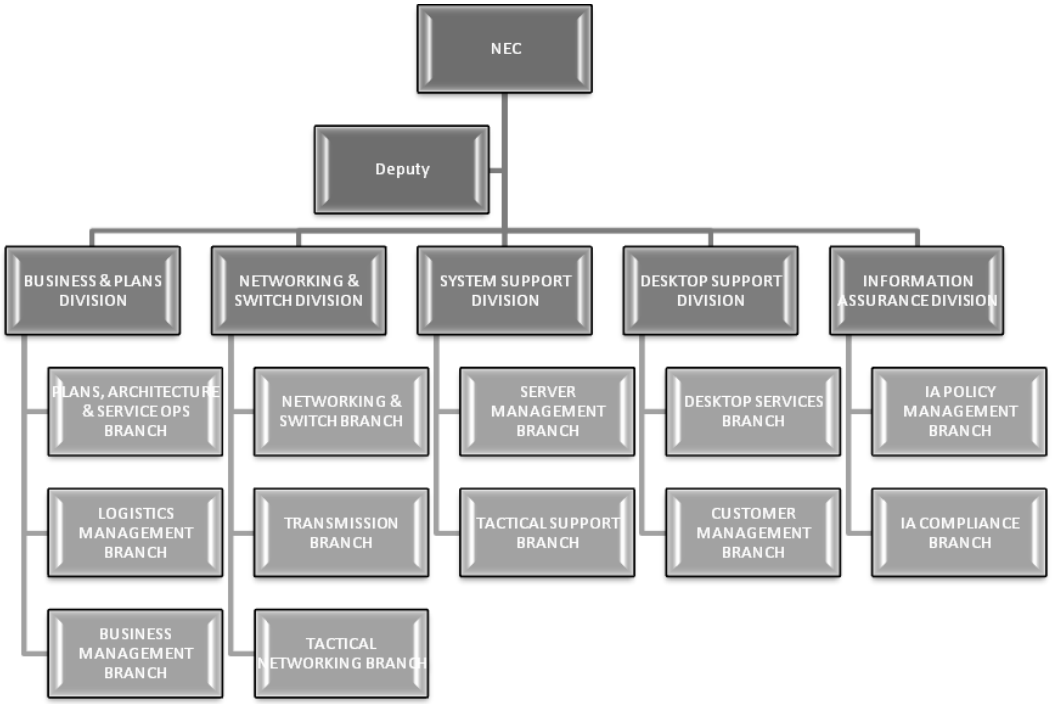

Figure 1: NEC Structure

Business and Plans Division. The business and plans division is responsible for NEC business operations in support of all operations, and all planning aspects in support of the installation to include logistics, budget, contracts, property, training, and policy and governance. This division also supports the installation by providing long-range planning for communications projects and oversight of quality control, quality assistance requests.

Network and Switch Division. The network and switch division is responsible for the entire installation network and for connectivity to the LandWarNet utilizing various circuits and means of connections to provide support to the installation. There are three branches in this division that play a key role in obtaining and delivering services; 1) The network and services branch is responsible for the wide area network, which includes NIPR and SIPR electronic mail, Local Area Network (LAN), Internet Access and COOP Implementation; 2) The transmission branch includes land mobile radio, cable installation, satellite, spectrum and voice and data; and 3) The tactical branch integrates warfighter systems, supports mobilization and conducts hardware and software training.

Desktop Support Division. The desktop support division has two branches that interact with users on the installations. The desktop branch is responsible for electronic mail (EMAIL), system administration, and end user desktop support and IP voice. The customer management branch executes service desk operations, problem management, customer relations, service request and customer training.

System Support Division. The support division is comprised of two branches the service management branch and the tactical support branch. These branches provide support for hardware and software, system administration, data base services and Web

services. The tactical branch is the integrator and assists with all the tactical integration of system hardware and software.

Information Assurance Division. The information assurance (IA) division has two branches, which include IA policy and management and IA compliance. The policy and management branch is responsible for the DoD information technology security certification and accreditation process (DISTCAP), enforcement reporting and IA training. The compliance branch covers operational reporting, scanning of the network, firewall management and compliance, proxy services, intrusion detection, antivirus servers, monitoring and COMSEC.

The Army has an ever-increasing demand for network connectivity and Information Technology (IT) at each CONUS location. Uniformed and government personnel require reliable and secure networks that enable operations in the joint and interagency environment. Today, these requirements do not meet the demands imposed upon them due to regulatory compliance and resource limitations. These resources include technical, operational, and managerial personnel, and equipment, to operate and safeguard the network. The provisioning of network services includes voice and data at each of the Army's posts, camps, and stations, utilizing Army owned and commercially leased circuits and equipment. A failure to allocate the proper amount of resources will cause network and subsequent mission failure.

C4IM Services

Organized into three categoriesC4IM baseline provides services to Army installations. The three service areas include Service 15, (Communications System and System Support), Service 18, (Information Assurance), and Service 19, (Automation). As well as further divided sub areas, which are critical to operations and provide a

viable network and connectivity, and support on Army installations at large. Service 15 includes telephone and data infrastructure, wireless infrastructure, emergency communications telephone service, video teleconference (VTC) services and secure VTCs to the tactical brigades, range and field telephone services, telecommunications COOP, communications service support, fire safety and other circuits and finally non-tactical radios and spectrum management services. Each of these services plays a critical role in bringing communications systems support to the entire installation.[14]

Service 18 (Information Assurance) includes DoD's Public Key Infrastructure (PKI) services, communications security (COMSEC) services, risk management/accreditation/certification services and network security services. Service 18 is critical to national defense and the security of the network. "While cyberspace relies on the digital infrastructure of individual countries, such infrastructure is globally connected, and securing it requires global cooperation."[15]

Service 19 (Automation) plays a key role for the enterprise. Data and collaboration are critical enablers for the warfighter during all phases of deployment, and they are essential in CONUS based installations. Service 19 includes mail/messaging/collaboration and storage services, database administration services, desktop/software/peripheral support services, web support services, file and print. Mission server support services includes support to the tactical units, management of data network services also SIPRNET to the tactical battalions, network continuity of operations plan (COOP), and automation, telecommunications, and network service support with 24/7 help desk support.

Current Network Challenges and Issues

Effective delivery of services to the warfighter requires a full understanding of the requirement along with a commitment of critical resources to enable mission accomplishment. A Department of the Army memorandum highlighted the fact that the NEC provides critical command and control functions for the LandWarNet. In light of this significant requirement, the Army must take a hard look at staffing and resource priorities for NEC operations, along with the established NEC information infrastructure. Until there is adequate investment to enable the NEC's critical role in supporting LandWarNet, Army C2 will suffer; the network remains at risk, and Net-centric operational goals and the transformation of operating processes remain unfulfilled."[16] Additional resources are also required to expand the network and meet the needs of the Army.

The greatest challenge for NECs is the delivery of C4IM services to an established standard. The established standards are in the C4IM service list, approved, and validated annually. There are over 470 different tasks in the current C4IM catalog (July 2010). The C4IM catalog describes the task, management decision package (MDEP), baseline, or mission funded, availability, response time, performance measures, capacity, and workload. An example is 15.1.1.2-provide dual tone multi-frequency (DTMF) type telephones. The MDEP is QUIM. It is a baseline service. The availability is 24x7 (less scheduled down time) with a response time for add and change within 5 days. The performance measure requires 98% reliability and the capacity is one per installation user.

Another significant challenge that Soldiers face today, is a lack of network connectivity, or inconsistent access to the network and information technology

resources, particularly during transitions from training to deployment and return to home station.[17] This is a challenge because the current C4IM baseline provides insufficient support for the generating forces in CONUS. Current individual command funding of IT products and services obscures total IT cost and funding for the Army. There is no single Army procedure or process to validate IT requirements, or accurately capture costs and track the amount of mission dollars expended to cover IT expenses. The Army will continue to have installations with more services than they need and others that struggle to provide services in accordance with published standards, if the deficiency not addressed.

Maintaining current operations with current levels of funding will require changing (lowering) the standards in the C4IM catalog. This will allow installations to operate at 100% of the newly established level, rather than to continue funding at the current reduced 60% level with heightened requirements. If this does not occur, mission commanders will continue to spend mission dollars to cover IT requirements at installations, which will continue to fragment the expenditures of scarce IT resources, and make accountability of funds expended difficult for the Army to capture and track.

Today the Army does not have the visibility or mechanisms in place to track C4IM and mission funded expenditures in CONUS.[18] It was determined that the C4IM baseline does not come close to meeting the units at the posts, camps and stations needs or requirements, which has caused commanders and installations in CONUS to commit mission dollars and other funds to cover costs associated with the network, along with reoccurring and habitual support. There are discrepancies in the level of C4IM services delivered to commands with similar requirements. Based on this

circumstance, some commands will supplement C4IM funding to raise service levels, while other, less well-funded commands accept an amber level of service.[19] Commands and organizations are covering the cost with mission dollars today but in the future, those dollars will not be available to pay for IT expenditures.

Current Army regulation allows for different funding streams for IT solutions in the form of centrally managed and command managed funds. [20] "The total cost of common and enhanced user services plus command-specific IT is estimated to be at 3.18 billion per year. For every dollar spent on C4IM baseline, commanders spend an additional estimated $ 0.30 to $1.50 or more enhancing these services or enabling command-unique IT."[21] The organizations that had signal personnel and equipment operating a portion of the network will now have to rely on some other organization to provide the services. These organizations may also have issues with the command relationships and the new way of receiving the communication services.

In FY 09, the amount of funding to provide the services from the MDEPs managed by the CIOG6 for 37 CONUS locations was 444.1 million; however, there was a total of 612.7million. In MDEPs, (MXCB, QOIM) there were shortfalls between the forecasted requirements, validated requirements and amounts actually funded and executed. Similarly, in FY 09, MEDCOM programmed 300 million dollars to cover Information technology expenses and spent over 600 million.[22] Both organizations develop programs and projects and request funding through the POM. In FY 10, CONUS NECs received about 72% of the required funding to deliver requested and required services to installations. This was not sufficient to cover the cost of required basic services, which drove organizations to pay for IT services out of mission dollars.

The Army G3 validated the DOIM model and approved the document for POM FY12-17. NETCOM must analyze the delivery of services to its CONUS customers and continue to allocate dollars for the services against the validated C4IM catalog. To provide services at the 37 CONUS locations, 5296 personnel are required to execute NEC operations. The approved manning document to program the dollars for personnel required and received approval validation for the FY12-17 POM in order to deliver the services required in the C4IM catalog. However, an example of the validated process against the requirement the FY11 Table of Distribution Allowances (TDA) authorizes only 3107 of the 5296 personnel required.

In order to mitigate the above-mentioned personnel shortfalls, some major commands such as Forces Command (FORSCOM), Army Material Command (AMC) and Medical Command (MEDCOM) provided resources to the CONUS based NECs to pay for service delivery. FORSCOM specifically provided 27 million dollars over two years for enhanced services at all FORSCOM locations. This funding allowed for the hiring of an additional 278 personnel at FORSCOM locations to enhance operations and conduct work in four new areas. The four new services included 24x7 Help Desk support; Secure Internet Protocol Router Network (SIPRNET) to the battalion headquarters locations; secure Video teleconferencing service support to the brigade headquarters locations; and support to the tactical users. These enhanced services will become part of the C4IM catalog as baseline services in FY12.

Recommendations

A comprehensive approach by the Army G3/5/7 LandWarNet is required to enable the Army to better provide network capabilities and overcome the challenges and issues outlined in this study. These changes must occur to address shortfalls in

organizational structure, resourcing, and current network support processes. These changes will also allow the Army to set conditions that allow the Army to meet the four strategic objectives currently aligned with the GNEC. Critical to this change effort is leveraging the C4IM catalog to capture validated requirements.

To enable networked capabilities and to enhance existing installation network requirements, the Army CIOG6 should create a C4IM catalog that actually reflects and supports the requirements of the 21st century warfighter and incorporates ways to capture required and future changes as mission requirements grow and evolve. The Army must allocate additional resources to enable additions to existing telephone services to include the addition of VOIP, SVOIP and comprehensive collaboration services. Adjustments made to existing cell phone resourcing protocols will support a shift in baseline usage.

Video Tele-Conferencing services must expand and provide secure VTC to existing baseline systems. Within this construct, each Army division will receive adequate resources for five secure systems and each brigade combat team allocated at least one secure system. Additionally bridging capability for video capability for every Army Command (ACOM), Army Service Component Command (ASCC) and Direct Reporting Unit (DRU) should increase to accommodate the greater demand. Finally, the Army must allow base and mission commanders to eliminate or reduce mission spending and allocate funds in support of C4IM requirements. Adding to this dilemma, the installation commanders will object to the loss of mission dollars to cover the demands of the network. Additionally, the loss of direct control over the network and of

those personnel operating it will cause concerns for the commander on the ground at each location.

In order to improve network defense, the Army must first resource the 7th Signal Command and subordinate NECs with the required personnel to enhance current initiatives and programs designed to defend the Network. Specifically, added personnel will allow the Army to provide the level of IT support to accomplish the Army's mission, meet critical needs, and ensure standards on the network. Simultaneously, the Army must continue to coordinate, and synchronize efforts with other governmental agencies to facilitate unity of effort and enhance interoperability.

In order to improve overall network effectiveness and realize efficiencies, the Army must first enhance the C4IM baseline and allocate resources such as force structure and funding to accomplish and meet mission requirements. This begins with the Army G3 completing and approving the validation process for enhanced network capabilities, to include adding additional services required by each installation to the C4IM catalog. In support of this process, existing funding must shift (reprogram) from mission commanders to NETCOM in order to cover additional identified requirements. Equipment acquisition and life cycle support, including end user devices, voice mail and other essential call features, to include conference call, must shift to a baseline requirement. User accounts for email service should change from 100 megabits (MB) to 1 gigabyte (GB). Additionally, the Army should introduce tiered levels of help desk support to become more responsive and provide 24/7 desk support for installations and the operating forces.

With respect to staffing, the Army must approve the request to authorize 80% of NEC staffing in FY 11. Similarly, to achieve enterprise solutions, the Army must build the POM for future years to cover the additional cost. The enterprise includes Enterprise Service Desk, Active Directory consolidation, Enterprise Network Operations, Common Operating Environment, and Enterprise Exchange Email. ASCCs, ACOMs and DRU commanders will benefit from having a single point of contact for IT requirements, local standards, service request procedures, cost data and when the NECs are fully manned, equipped and organized.[23]

In pursuit of ensuring enhanced interoperability, the Army should consider synchronizing standard levels of services across commands, as they apply to mission specific requirements associated with each major command and agency. In support of this modification, the Army G3 should create a network validation process to capture changes and update to service list. Provided and included in the C4IM catalog are any additional resources required in support of this effort. Also, captured as a change to the C4IM catalog are all additional enhancements and new types of services in support of commanders' requirements at each installation.

The Army must provide the amount of resources to NETCOM for the NEC, or, it must change the requirements in the C4IM catalog. In order to consider the network a warfighting platform, the Army must allocate resources to cover those validated requirements. Personnel serving the government have obtained IT services such as telephone connection and EMAIL service from non-DoD providers for many years.

The Chief of Staff of the Army has directed that the LandWarNet be transformed into a centralized, more secure, and sustainable network, capable of supporting an

expeditionary Army and making daily operations more efficient.[24] Educating the organizations who rely on the network, validating and resourcing the requirements and moving to enterprise services will allow for the desired end state of the DoD leadership.

Conclusion

To overcome the challenges of future requirements for information dominance, the Army must develop a strategy that ensures organizations have access to global networks and required services throughout any area of operation. The Army network strategy objective is to deploy an integrated network, which spans all echelons of command and supports Army, Joint and Coalition operations. The networks will support both the Operating and Generating Forces and share information across various levels of classification. Everyone must understand that the networks have not been resourced to the level expected or required which has caused shortfalls in the current posture. NECs do not have the capability to transition to new technology to provide data increased storage, network collaboration, and to assistance the unit leadership on integration of command and control equipment. It is the responsibility of the signal community, including the NECs, to gain the trust and confidence of all those who rely on the Network, that it can be delivered in a safe, secure, and reliable manner and at an affordable cost by one organization in CONUS. As NETCOM and 7th Signal Command deliver the network services and show the efficiency over time, the trust and confidence will be earned.

Today, the budget allow for commands to provide funding for the networks but if the LandWarNet is not realized, requirements not documented and validated, resources allocated for IT the NECs will continue to struggle to provide an available, reliable, and secure network. Changing technology and new requirements at each location may

cause or be a factor in the delivery of communications services. Having a commanding officer who is responsible for the Networks in CONUS with two brigades is now improving the Command and Control (C2) aspects, giving the senior commander someone to whom he or she can communicate his or her requirements for each installation. With the additional resources allocated to 7th Signal Command, along with the validated and resource requirement, the sole provider of network services will facilitate the integration of the NECs' personnel at each of the locations alongside senior personnel identifying the validated requirement. Efficiency of expenditures must be the mantra for all of us in the future.

Endnotes

[1] Barack Obama, National Security Strategy,(Washington DC: The White House, May 2010, 22

[2] Barack Obama, National Security Strategy,(Washington DC: The White House, May 2010, 8

[3] Barack Obama, National Security Strategy,(Washington, DC: The White House, May 2010, 4

[4] Janet Napolitano, Bottom-up Review Report, Washington DC: Homeland Security, February 2010), X

[5] Capstone Concept for Joint Operations, Version 3.0, 15 January 2009, 4

[6] Capstone Concept for Joint Operations, Version 3.0, 15 January 2009, 21

[7] DA IG Report Fiscal year 2009

[8] CIOG6, Transforming LandWarNet, Implementing the Enterprise Strategy, August 2010, 4

[9] Army CIOG6, Transforming LandWarNet, Implementing the Enterprise Strategy, August 2010, 4

[10] U.S Department of the Army, Information Management, Army Knowledge Management and Information Technology, Army Regulation 25-1, (Washington D.C:, Department of the Army, December 4, 2008), 33

[11] The Army Mission Command Portfolio Modernization Strategy, 22 September 2010, 2

[12] Army CIOG6, Transforming LandWarNet, Implementing the Enterprise Strategy, August 2010, 4

[13] Standard NEC Structure Brief to BG Jennifer Napper, Commanding General, 24 June 2009

[14] CIOG6 POM12-17 Priority (NECs), Resourcing NECs to Deliver C4IM Services at Amber C2 Level

[15] National Security Strategy, May 2010, 50

[16] General Benjamin Griffin, General Dan McNeill, LTG Anthony Jones, " Re-alignment of Director of Information Management (DOIM) Organizations," memorandum for Vice Chief of Staff, United States Army, Washington, DC, October 2005

[17] Army CIOG6, Transforming LandWarNet, Implementing the Enterprise Strategy, August 2010, 3

[18] Army Audit Agency report, 14 July 2010

[19] CIOG6 POM12-17 Priority (NECs), Resourcing NECs to Deliver C4IM Services at Amber C2 Level

[20] BRAC Summit VII, Army standard for IT Common Levels of Support (SICE) Brief, 3 November 2010

[21] CIOG6 POM12-17 Priority (NECs), Resourcing NECs to Deliver C4IM Services at Amber C2 Level

[22] Barzie Drewry, E-Mail message to Author, November 12, 2010

[23] 7th Signal Command, Briefing for NEC Course, 22 June 2010, BG Jennifer Napper, Commanding General

[24] Draft HQDA EXORD, LandWarNet-Global Network Enterprise Construct (GNEC) Implementation-Army Migration to DOD Enterprise Email Services, 29 Oct 2010